Contract Clause Guide for Unclassified Information System Security Systems and Services

A Mandatory Internal Reference for ADS Chapters 302 and 303

Revision Date: 08/21/2006
Responsible Office: M/OAA/P
File Name: 302mah_082106_cd45

Functional Series 300 **INTERIM UPDATE 03-03**
Acquisition and Assistance

SUBJECT: Contract Clause Guide for Unclassified Information System Security Systems and Services

NEW MATERIAL: Attached is the new Information System Security (ISS) Contract Clause Guide for the acquisition of systems and services, a Mandatory Reference for ADS 302, USAID Direct Contracting; ADS 303, Grants and Cooperative Agreements to Non-Governmental Organizations; and ADS 545, Information Systems Security.

EFFECTIVE DATE: 02/28/2003

POLICY

USAID/General Notice
M/IRM/OD and M/OP
03/25/2003

Subject: Contract Clause Guide for Unclassified Information System Security Systems and Services

Attached is the new Information System Security (ISS) Contract Clause Guide for the acquisition of systems and services, a Mandatory Reference for ADS 302, USAID Direct Contracting; ADS 303, Grants and Cooperative Agreements to Non-Governmental Organizations; and ADS 545, Information Systems Security.

Information system security (ISS) is the protection of the integrity, availability, and confidentiality of automated information and the resources used to enter, store, process, and communicate the information. Office of Management and Budget (OMB) Circular A-130 requires USAID to incorporate ISS into its information systems and services acquisition process.

This Mandatory Reference is a collaborative document produced by the Office of Information Resource Management (M/IRM) and the Office of Procurement (M/OP), and provides guidance on including ISS requirements in the acquisition of information systems and services. This Guide is designed to support Agency procurement initiators, Contracting Officers (COs), Cognizant Technical Officers (CTOs), designated Information System Security Officers
(ISSOs), and other procurement officials and their staff.

Points of Contact: Procurement questions concerning this Notice may be directed to Diane Howard, M/OP, (202) 712-0206. Other questions may be directed to Evelyn Hogue, M/IRM/IPA, (202) 712-5046.

Notice 0337

The Contract Clause Guide For Unclassified Information System Security Systems and Services file starts on the next page.

File name	Notice Date	Effective Date	Editorial Revision Date	ADS CD No.	Remarks
Iu3_0303_033103_cd31	03/25/2003	02/28/2003		ADS CD 31	
302mah_082106_cd45	03/25/2005	02/28/2003	08/21/2006	ADS CD 45	This IU has been turned into a mandatory internal reference: 302mah.

Mandatory Reference: 302, 303, 545
File Name: 545mah_022803_cd31
First Issuance: 02/28/2003
Effective Date: 02/28/2003

Contract Clause Guide
For Unclassified Information System Security
Systems and Services
A collaboration between M/IRM and M/OP

I. Introduction

Information system security (ISS) is protection of the integrity, availability, and confidentiality of automated information and the resources used to enter, store, process, and communicate the information. Office of Management and Budget (OMB) Circular A-130 requires agencies to incorporate ISS into their information systems and services acquisition process.

This Contract Clause Guide is a mandatory reference for ADS 545, Information Systems Security; ADS 302, USAID Direct Contracting; and ADS 303, Grants and Cooperative Agreements to Non-Governmental Organizations; and provides guidance on including ISS requirements in the acquisition of information systems and services. ISS requirements include those that govern system features and operation, and those that govern the behavior of contractors in the development and/or maintenance of these systems. The Guide is designed to support Agency procurement initiators, Contracting Officers (COs), Cognizant Technical Officers (CTOs), designated Information System Security Officers (ISSOs), and other procurement officials and their staff.

The integration of ISS into Federal Information Processing (FIP) procurement will result in improvements in 1) meeting Agency goals and program objectives, 2) protecting Federal assets, and 3) protecting individual rights. This integration is accomplished by incorporating ISS into all phases of the procurement cycle:

Planning,
Solicitation and award, and
Administration and closeout.

II. Scope

This Guide applies to all contracts, regardless of the source of funding, when the contracted systems or services will be connected to, or require the use of, a USAID general support system (GSS) in USAID/Washington (USAID/W) or at the Missions. The Guide can also be applied whenever a requestor, an acquisition or contracting

authority, or the cognizant designated ISSO believes it would be in the best interest of protecting USAID's information systems.

The terms "contractor" and "contractor personnel," as used in this document, apply to non-Personal Services Contractors (PSCs) and subcontractors, including but not limited to commercial entities, non-profit organizations, educational institutions, and individuals. U.S. citizen and foreign service national PSCs are subject to the same rules and restrictions as USAID direct-hire employees.

Assistance instruments (grants and cooperative agreements) awarded to non-governmental organizations (see ADS 303, Grants and Cooperative Agreements to Non-Governmental Organizations, and ADS 304, Choice of Implementation Instrument) should not, typically, support the recipient organization having access to the USAID General Support System (GSS) AIDNET. If the unique nature of the program USAID is supporting through the grant or cooperative agreement justifies the recipient organization having such access, then the sponsoring office must obtain the approval of the Agency ISSO (see ADS 545.2.e) before the recipient is granted access. If the Agency ISSO approves access, the procedures in this Guide apply to the recipient on the same basis as contractors. Agreement Officers must therefore adapt the contract clauses in Section VII of the Guide as needed to include language appropriate for assistance awards.

III. References

The guidelines in this document were adapted from the guidance in the National Institute for Standards and Technology (NIST) Special Publication 800-4, Computer Security Considerations in Federal Procurement, and NIST Interagency Report NISTIR 4749, Sample Statements of Work (SOWs) for Federal Computer Security Services. Procurement personnel should use these references as detailed guidelines for a more in-depth understanding of Federal requirements for ISS and to support the preparation of contract wording. This will ensure ISS compliance in the acquisition of complex information systems (IS) products and services. USAID's policies on security for unclassified information system assets are prescribed in ADS 541, Information Management, ADS 545, Information Systems Security, and their associated references.

This USAID contract clause guidance augments the Agency's Acquisition Regulation (AIDAR). The AIDAR contains requirements for all USAID contractors, subcontractors, and PSCs to comply with USAID policies in safeguarding unclassified, including Sensitive But Unclassified (SBU), USAID data held, processed, or transmitted via information systems within or connected to USAID. This contract clause guidance implements USAID's acquisition-related aspects of Federal policies for ensuring the security of unclassified information system resources. For additional guidance, questions, and clarification concerning the information in this guide, please contact the Bureau for Management, Office of Procurement, Policy Division (M/OP/P) or the ISS security team at **securitytraining@usaid.gov**.

IV. Roles and Responsibilities

A team-based approach to product and service procurements is improving acquisition success throughout the government. Adding ISS representatives to these teams will help ensure that ISS goals in systems and services are achieved. The following USAID officers have specific ISS responsibilities in the development and management of contracts for or that include the acquisition, operation, and maintenance of USAID IS products and IS services.

A. Chief Information Officer

The USAID Chief Information Officer (CIO) ensures that the ISS requirements of OMB A-130 and other applicable Federal regulations and Agency policies are met for all Agency IS acquisition and maintenance contracts.

B. Information System Security Officer

The USAID Information System Security Officer (ISSO) ensures that the ISS requirements of OMB A-130 and other applicable Federal regulations and Agency policies are met for the acquisition, operation, and maintenance of all Agency GSS and for major applications that interface with the GSS. The ISSO for USAID must ensure that appropriate ISS safeguards are incorporated into the staffing, design, specification, development, testing, and acceptance of these systems and related IS services. The USAID ISSO's ISS duties and responsibilities are specified in ADS 545.

C. Contracting Officers

USAID Contracting Officers (COs) must ensure that appropriate ISS requirements are accurately specified, funded, and enforced for all USAID IS acquisition, operation, and maintenance contracts under their supervision.

D. Cognizant Technical Officers

USAID Cognizant Technical Officers (CTOs) (or Contracting Officers Technical Representatives (COTRs)) have a key role in ensuring that cost-effective ISS processes and features are incorporated into IS products and services. CTOs represent the product or service requestor in the acquisition process. They understand both the technology associated with the acquisition and the requestor's objectives. They ensure that these factors are married in a way that meets USAID's business goals and security requirements, and they oversee contractor performance. CTOs also lead the development of sensitivity assessments for the systems and data associated with the contract and work with the designated ISSO to ensure that the appropriate levels of protection are applied to the contract. The information and contract clause examples in this Guide are designed to assist in achieving these requirements. CTOs who support program acquisitions that are not under the responsibility of a designated ISSO may contact the ISS security team at **securitytraining@usaid.gov**.

E. System or Service Requestors

Information systems or services requestors must understand that these acquisitions have to include ISS specifications appropriate to the system or service's application in the Federal and USAID IS operational environment. Requestors must include the appropriate designated ISSO(s) and/or CTO(s) (if the requestor is different than the CTO) during the preliminary planning for the system or service and throughout the acquisition process, especially in view of the exponentially escalating technical complexity of and security threats associated with new information systems.

F. Designated Information System Security Officers

USAID designated ISSOs ensure that the ISS requirements of Agency ISS operational and acquisition policies are met for

The development, operation, and maintenance of systems for which they are the designated ISSO, and
Systems that interface with their Mission and/or USAID GSS.

Designated ISSOs, as the information security representatives of their system or organization, assist acquisition officials with both a system's security features and the security associated with the processes and people involved in the acquisition.

V. Task Examples Requiring Security Provisions

ISS must be addressed in all contracts that include Information Technology (IT) resources or services in which a contractor must have physical or electronic access to USAID's sensitive information contained in unclassified systems that directly support the Agency's mission. This includes IT hardware and software, and the services associated with the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.

Examples of contract tasks that require security provisions include

Access to USAID's Privacy Act-protected data, legally protected data (including source selection information as described in FAR 3.104), financial data, or any commercial data that is proprietary to a third party entity;

Acquisition, transmission, or analysis of data owned by USAID with significant replacement costs should the contractor's copy be corrupted; and

Access to USAID networks or computers at a level beyond that granted to the general public.

The contractor must not use or redistribute any USAID information processed, stored, or transmitted by the contractor except as specified in the contract.

VI. Information System Security in the Acquisition Cycle

The application of USAID's ISS policy and best security practices must begin during the concept development of a new system or service and continue through system or service delivery and acceptance.

A. Planning Phase

The first phase in the acquisition cycle is planning, and it must include ISS considerations.

1. Sensitivity Assessment

During the initial planning phase of the acquisition cycle or task order development, the definition of the security requirement for the product or service being procured should begin with a preliminary sensitivity assessment. This sensitivity assessment should be led by the individual who will have the best understanding of the proposed system's technology and technical environment, and its intended application in USAID operations. Usually, this individual will also be designated as the CTO for the acquisition. The CTO must also initiate a sensitivity assessment if the need arises at any time during the acquisition cycle.

The sensitivity assessment should result in a brief qualitative description of the basic security needs in terms of the need for integrity, availability, and confidentiality. Legal implications, Federal policy, Agency policy, and the functional needs of the system or service determine data sensitivity. Factors including the importance of the system or service to the USAID mission and the consequences of unauthorized modification, unauthorized disclosure, or unavailability of data must be considered when assessing sensitivity. In this phase a determination may be made as to whether the system will be treated as a GSS or major application (MA). Such systems normally require additional security considerations such as preparing a security plan and naming a designated ISSO for the system.

The sensitivity assessment must include an examination of contract staffing profiles to ensure that there is a clear "separation of duties" throughout the contracted system's development and operational cycles and for any IS services contracted. Separation of duties ensures that no single person has the ability to manipulate the hardware, software, or processing of a system to commit fraud or to waste or abuse USAID systems without the oversight of another person. One example of role conflict could be a contractor's ability to request, award, and pay for a product or service without another person's review and approval. Sensitivity assessments must also consider the concept of "least privilege," where individual contractors or groups of contractors have access

only to the systems and data required for their tasks, not “broad” system privileges that may put USAID’s information at undue risk.

2. Requirements Analysis

A requirements analysis is an in-depth study of the need for the system or service. The following ISS components must be included in a requirements analysis:

An analysis of integrity, availability, and confidentiality requirements;
An updated sensitivity assessment;
An analysis of the level of assurance required;
A planning phase risk analysis; and
A preliminary certification and accreditation (C&A) plan that will be used to ensure that the system meets the Agency’s ISS requirements and receives approval to operate.

These analyses present a conceptual framework for ISS planning and should include participation by the ultimate functional group user and ISS staff to ensure that operational and security requirements are addressed accurately and in sufficient detail.

3. Other Planning Components

Other parts of the planning process that should incorporate ISS include the following:

Feasibility study,
System cost-benefit analysis,
Software conversion study (if appropriate),
Analysis of technical alternatives, and
Market surveys.

If security is not addressed comprehensively in the planning cycle and throughout the system’s life cycle, the system or service could be acquired or operated without cost-effective security solutions.

B. Solicitation and Award

In the second or solicitation and award phase of the acquisition cycle, requests for proposals (RFPs) are developed and issued, proposals are received and evaluated, and awards are made. An RFP can be a flexible document that allows for substantial creativity. Because of this flexibility, it is impossible to address a precise mapping of ISS considerations into the uniform solicitation. The procurement initiator must decide how the ISS considerations will be met given the many options the RFP may provide. Security requirements can be included in the statement of work (SOW) as specifications, tasks, labor, work, level of effort, etc. The procurement initiator should concentrate on what is required and work with the CO to determine how to ask for it.

1. General Specifications

Considerations for general ISS specifications are contained in guidance from NIST, DoD, other Federal agencies, and commercial groups. Each specification must be justified from the requirements analysis and testable to ensure conformance. Safeguards recommended by a general source should be considered, but they should not be included in an RFP if the risk analysis does not support them.

2. Federally Mandated Specifications

Federally mandated or directed ISS specifications are those that are required by law to be included in an RFP. USAID and other executive agencies must comply with OMB Circular A-130 and its Appendix III. USAID-specific directed specifications are contained in ADS 545, Information Systems Security. These are official policy directives issued with the concurrence of Agency legal and procurement officials. It is very important to be aware of directed specifications, and Agency ISS staff should assist in determining whether or not an RFP addresses them accurately. If a specification in an RFP conflicts with a directed specification, a waiver must be obtained from the organization responsible for the directed specification (e.g., an ADS 545 specification is the responsibility of the Bureau for Management, Office of Information Resources Management, Information Policy and Administration Division (M/IRM/IPA)).

3. Evaluation

An evaluation determines if an offer meets the minimum requirements described in the RFP and assesses the offeror's ability to successfully accomplish the prospective contract. This can be difficult when evaluating ISS features. Offerors must provide assurance that hardware and software claims regarding ISS features are true and that they can provide the proposed services. Security personnel need to be sure they are asking for the information they really need to ensure that the government is not later liable for the cost of additional assurance that may be required.

The requesting office or CTO (if different from the requesting office), working with the ISSO and the CO, must develop and use an evaluation plan and solicitation instructions that provide information to offerors on how the ISS features of the proposal will be evaluated. This includes information on security acceptance testing.

Testing can be part of the evaluation or part of the post-award acceptance. The USAID and/or contractor test and evaluation team must ensure all system testing is done with all required security features enabled. Evaluation criteria may not be modified after proposals are received unless the CO amends the solicitation (see FAR 15.206). Procurement initiators must be sufficiently aware of the marketplace to develop an effective security features evaluation plan for the RFP.

4. Source Selection

Source selection is the determination of a successful offeror. ISS considerations incorporated during the planning and solicitation phases will be part of the evaluation and source selection. An individual with extensive ISS experience should be part of the evaluation and selection team.

C. Administration and Closeout

Administration and closeout is the final phase of the procurement process. Two important ISS functions during this phase are acceptance and monitoring contractor performance. Acceptance must be predicated on the comprehensive and successful testing of the system's ISS features. Acceptance does not, however, equate to approval to operate. While related to acceptance, approval to operate is a separate decision based on the risks and advantages of the system. For more information on approval to operate, see ADS 545.3.7.2, System Certification.

Contractor performance must be monitored throughout the system life-cycle to be sure security has not degraded over time and that changes in the environment or system that result in new vulnerabilities are recognized and appropriate safeguards are put in place. This is a key role for the designated ISSOs of GSS and major applications.

VII. ISS Contract Terms

This section provides language to be used in the applicable sections of the uniform contract format (see FAR 15.204-1) of RFPs and contracts to ensure that the requirements for ISS contained in this Guide are incorporated. The first part of each section below contains the prescriptions for when and how to use this language, and the actual recommended RFP/contract language follows. This language is intended as a source of general specifications and should be tailored by contracting, requiring office, ISS, and Office of Security (SEC) staff collaboratively and as necessary to reflect the specific ISS requirement of each system or service.

Because it is subject to tailoring, variations to this language that still comply with this Guide do not require a deviation as specified in ADS 302 and its Mandatory Reference, AIDAR 701.4. However, no deviation may be made to the policy and essential procedure in section 302.5.3 and E302.5.3.

When a deviation is necessary, the responsible USAID CO initiates an Action Memorandum to the Head of the Contracting Activity (HCA), obtaining any clearances and approvals required by the HCA. This deviation request Action Memorandum must comply with the procedures in AIDAR 701.470 and be submitted sufficiently in advance of the requested effective date of the deviation to allow all involved parties adequate time to consider and evaluate the request.

If the Agency ISSO approves a grant or cooperative agreement recipient to have access to a Mission or the Agency's GSS, the Agreement Officer must include the following clauses in Section VII.A.4 below, altered as appropriate to be assistance provisions, into the award document.

A. All System Developments and Services

This section prescribes general ISS requirements for COs to include in Section H, Special Contract Requirements, of solicitations and contracts.

1. General ISS Clauses

a. Designation of ISSO. OMB Circular A-130, Appendix III, and USAID policy require that the ISS responsibilities for USAID GSS and major applications be assigned by name to a U.S. citizen employee (either a direct-hire in USAID/W or a U.S. citizen employee or PSC overseas). COs must clearly state the name and location of the responsible person in all contracts associated with these systems.

b. Contractor's General ISS Responsibilities. Contractors must understand their general ISS responsibilities for USAID systems. The language in Section VII.A.4 of this Guide is to be included in Section H of the RFP/contract if all or any part of the contract includes IS resources or services that require the contractor to have physical or electronic access to USAID's sensitive information contained in unclassified systems that directly support the Agency's mission. This includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. References to requirements in other ADS Chapters or Federal policy documents (e.g., OMB Circular A-130) may also be added into this Section H language if applicable to the system or service acquisition.

c. Limitation of Use of USAID Information. The contract terms must emphasize the contractor's limited ability to use USAID information. The language in Section VII.A.4 may be used for this purpose. However, while effective in limiting the contractor's use of USAID information, before using this language the CO, CTO, and ISSO must be careful to ensure that all possible contractor information needs are specified.

2. Contractor Personnel Security

People constitute the most serious threat to USAID's information systems. Their actions, intentional or unintentional, can seriously interrupt or damage USAID's business operations and place personnel and other resources at great risk. This personnel risk is reduced through the application of a variety of examinations that support the assessment of an individual's suitability for access to USAID's IS. The breadth and depth of these examinations help determine the level of system access that may be appropriate for various contractors or groups of contractors.

Requesting organizations and data owners have the best knowledge of the sensitivity and risk associated with the information related to their acquisition of material or services. Working with their designated ISSO, CTO, and SEC representative, requesting organizations must determine the level of examination and acceptance that will be applied to the contractor personnel who may have access to their sensitive data and/or systems.

ADS 545, Section 545.3.3, Personnel Security Requirements for Access to Unclassified IS, provides the requirements for access to USAID unclassified information systems. At a minimum, any contractor granted access to a USAID system or network must have an employment authorization granted by SEC. More extensive personal examinations or investigations may be required at a level appropriate for the information to be accessed. SEC will assist requestors and CTOs in determining the type and level of investigation and authorization required for the security of the various categories of USAID information.

USAID's most valuable ISS tools are user security awareness, user knowledge of ISS requirements, and user behavior expectations at USAID. Users gain this knowledge initially by taking USAID's new user awareness and training programs, available in bi-weekly classes and on the USAID intranet. All USAID and contractor personnel system users must reinforce their knowledge annually by taking the ISS awareness training course on the intranet.

Contractors must apply the concepts of "separation of duties," "need to know," and "least privilege" in all contractor personnel assignments. USAID CTOs and designated ISSOs must ensure that contractors employ these security precautions. Separation of duties ensures no single person has the ability to manipulate the hardware, software, or processing of a system to commit fraud or to waste or abuse USAID systems without the oversight of another person. Need to know limits contractors' access to only that information required to perform their roles. Least privilege limits access to only those systems, networks, and files essential for contract performance. Compliance with and knowledge of these tools and concepts is required before any information system access is granted.

The application of these tools and concepts is especially important if contractor personnel will have access to USAID or other government Sensitive but Unclassified (SBU) information that requires an extra measure of protection. COs are to include the relevant paragraphs in Section VII.A.4 into the contract. This language states the personnel security requirements and will help to ensure that contractors are aware of these requirements and the expected ISS behavior of their staff while designing, developing, using, and maintaining USAID systems.

3. Contractor Facility Security

USAID contractors using non-USAID facilities and information systems to provide products or services to USAID are expected to provide the degree of security protection commensurate with the sensitivity of the USAID system access and information used for contract performance. CTOs, designated ISSOs, and SEC must collaborate to ensure that appropriate contract specifications for ISS are provided to the CO to include in the resulting contract, to protect USAID information resources in the contractor's environment.

4. Language for RFP/Contract Section H, Special Contract Requirements

As prescribed in Sections VII.A.1, .2, and .3 above, the following ISS language is to be included in Section H, Special Contract Requirements. COs may tailor this language as needed, provided that any variations are not inconsistent with Section VII.A, ADS 545, and ADS 545 references.

H.X Information System Security

H.X.a. *Designation of the Information System Security Officer*. The Contracting Officer hereby designates _____, located at _____, as the Information System Security Officer responsible for information system security for this system.

H.X.b. The contractor is responsible for the information system security of all systems used by the contractor, and connected to USAID networks, or operated by the contractor for USAID, regardless of location. The policy governing these responsibilities is USAID Automated Directives System (ADS) Chapter 545, Information Systems Security.

H.X.c. The contractor must not use or redistribute any USAID information processed, stored, or transmitted by the contractor except as specified in the contract.

H.X.d. All contractor personnel requiring access to USAID information systems, networks, or data must comply with the USAID Personnel Security Requirements for Access to Unclassified Information Systems policy requirements of the USAID Automated Directive System (ADS) Chapter 545. Contractor supervisors must ensure a sufficient separation of duties to prevent a single individual from committing fraud with, or abusing, USAID systems or data. Contractor personnel should also have access only to that information required for their tasks. Contractors must therefore request and enforce only those facility and information system accesses that are essential for each individual's job performance.

H.X.e. All contractor personnel with access to USAID information systems, networks, or data must complete a USAID-approved computer security awareness class and accept

the requirements of the USAID ISS rules of behavior before being granted access to USAID systems, and annually thereafter.

H.X.f. All contractor personnel must complete the security processes and meet the requirements specified by the USAID Office of Security for the sensitivity or classification level of the information for which they will require access.

B. Hardware, Software, and Services Procurements at USAID/W and Missions

1. System Design and Development

a. ISS procurements for the design and development of USAID GSS or major applications require the preparation and maintenance of an ISS Plan as specified in OMB Circular A-130, Appendix III, and ADS 545. After reviewing the prescriptions in sections VII.B.1, .2, and .3, and coordinating with the CTO and ISSO, COs are to include the applicable language from Section VII.B.4, tailored as needed, in the appropriate section of the RFP and contract.

b. Additional reference documents may be appended to this language if essential to the system development. However, coordinating and communicating a common "interpretation" of additional references among the government and prospective contractors and subcontractors may not be cost effective.

c. The USAID ISSO may also determine that a contractor must prepare an ISS Plan for other information system developments when this plan is in the best interest of USAID. If this is the case, the USAID ISSO will request that the CO responsible for that particular contract take the appropriate action to incorporate this requirement into the contract.

d. When an ISS Plan is not required, all contractors and subcontractors must still assure USAID that they will adhere to the ISS policies and procedures provided in ADS 541, Information Management, ADS 545, Information Systems Security, and their Mandatory References.

2. System Modifications, Operations, and Maintenance

ISS procurements for the modification, operation, and/or maintenance of existing USAID GSS, major applications, or Mission systems must reflect the requirement of adhering to the current ISS Plans for those systems and Missions.

3. Information System Security (ISS) Plan Development

The contractor may be required to develop and maintain an ISS Plan, in accordance with ADS 545 and its associated references, for systems for which the contractor has primary operational responsibility on behalf of USAID. This plan must describe the processes and procedures that will be followed to ensure appropriate security of IT

resources that are developed, processed, or used under this contract. The plan must also describe those parts of the contract to which it applies. ISS Plans must demonstrate a thorough understanding of ADS 541 and ADS 545 policy requirements. They must include, as a minimum, security measures and program safeguards to ensure that the information system resources developed, acquired, operated, maintained, and/or used by contractor and subcontractor personnel provide the following:

a. Protection from unauthorized access, alteration, disclosure, or misuse of information processed, stored, or transmitted;

b. Continuity of information systems (IS) support for USAID Missions, organizations, programs, and functions;

c. Management, operational, and technical controls sufficient to provide cost-effective assurance of the systems' confidentiality, integrity, and availability;

d. Appropriate technical, personnel, administrative, environmental, and access safeguards;

e. A virus protection program for all IS resources under their control;

f. A network intrusion detection and prevention program for all IS resources under their control; and

g. A continuity of operations plan in the event of a major system failure or disaster.

The CO must obtain the concurrence of USAID's ISSO before granting contractor requests for a waiver of any ISS requirements associated with an ISS Plan.

Additional information on the development of ISS Plans can be found in NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, and on the USAID M/IRM/IPA ISS intranet web site at **http://inside.usaid.gov/M/IRM/ipa/iss/progmgmt/secplan/main.htm**. The USAID ISS web site also provides access to an automated tool to assist in ISS Plan development.

4. RFP/Contract Provisions

a. ISS Plans – Submitting the ISS Plan with the Proposal

If an offeror is to prepare an ISS Plan as part of its proposal to be evaluated with the rest of the proposal as part of the source selection process, the CO must

Include this requirement in the RFP's Section C, Description/Specifications/Statement of Work. Suggested language follows:

The Contractor must provide, implement, and maintain an Information System Security Plan for the _____ system. The ISS Plan must comply with OMB Circular A-130, Appendix III, and USAID ADS Chapter 545, Information Systems Security.

Include instructions for preparing the ISS Plan in the RFP's Section L, Instructions, Conditions, and Notices to Offerors or Respondents. These instructions should be consistent with and, if necessary, supplement the guidance in Section VII.B.3 above; and

Include an evaluation factor to reflect the relative importance of the ISS Plan in Section M, Evaluation Factors for Award.

The requesting office/CTO and ISSO must provide these instructions and the evaluation factor as part of the contract specifications or work statement in the procurement request.

b. ISS Plans – Submitting the ISS Plan as a Contract Deliverable

If the ISS Plan is to be delivered at some date after contract award, the CO must include the following in the solicitation:

In Section C, include the suggested language in Section VII.B.4.a. above and add the following paragraph:

This plan must describe the processes and procedures that will be followed to ensure appropriate security of information system resources and data that are developed, processed, or used under this contract. The plan must describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan must be compliant with Federal law, OMB Circular A-130, USAID ADS Chapter 545, Information Systems Security, and Chapter 541, Information Management, and the recommendations in the National Institute of Standards and Technology (NIST) Special Publication 800-18.

In Section F, Deliveries or Performance, include the following deliverable:

F.X. ISS Plan. Within ____days after contract award, the contractor must submit for USAID approval an Information System Security Plan.

c. No ISS Plan Required

When an ISS Plan is not required, the CO is to include the following paragraph after the contract's Section H ISS language (recommended in Section VII.A.4 above):

H.X.g. By accepting the award of this contract, the contractor assures USAID that all contractor and subcontractor personnel will comply with the policy and procedures of the USAID ADS Chapter 541, Information Management, Chapter

545, Information Systems Security, their Mandatory References, and any future ISS policy changes or enhancements.

d. System Modifications, Operations, and Maintenance

When Section VII.B.2 applies, the CO is to include the following in Section H of the contract:

H.X.g. *[Note: this paragraph will not be included in the same contract as the provision in c. above*] The Contractor must adhere to the requirements and procedures of the current Information System Security Plan of the _____ system (or Mission), dated _____, unless exceptions are granted by the ISSO for USAID.

VIII. Additional Resources

[Note: This section may be used for additional reference guidance that may be electronically linked or provided as hardcopy attachments to this document.]

302mah_082106_w082806_cd45